CSCI 1515 Applied Cryptography

This Lecture:

- BFV: SWHE from RLWE (Continued)
- Private Information Retrieval

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from RLWE (BFV)

Step 2: Bootstrapping

Ring LWE (RLWE) Assumption

Polynomial ring $R = \mathbb{Z}[x] / (x^m + 1)$ where $m = 2^k$

↑ polynomials with integer coefficients modulo $(x^m + 1)$

$$R_q = \mathbb{Z}_q[x] / (x^m + 1)$$

↑ polynomials with integer coefficients modulo q and $(x^m + 1)$

χ : "noise" distribution over R

$a \xleftarrow{\$} R_q \qquad s \xleftarrow{\$} R_q \text{ (or } s \leftarrow \chi) \qquad e \leftarrow \chi$

$$(a,\ [a \cdot s + e]_q) \overset{c}{\simeq} (a,\ b \xleftarrow{\$} R_q)$$

SWHE from RLWE (BFV)

Plaintext space $R_t = \mathbb{Z}_t[x]/(x^m+1)$ $\quad \Delta := \lfloor \frac{q}{t} \rfloor$ $\quad t \ll q$

Ciphertext space $R_q \times R_q$

Gen:

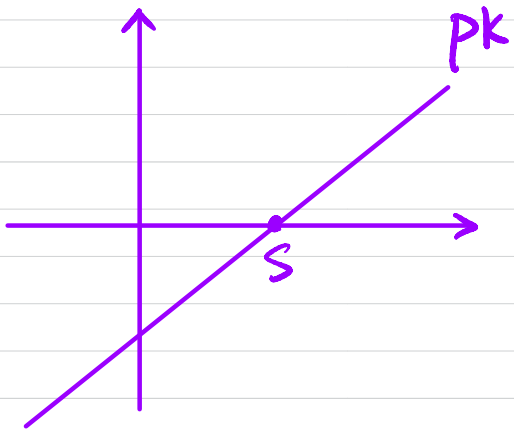
Sample $a \xleftarrow{\$} R_q$ $\quad s, e \leftarrow \chi$

$sk = s$

$pk = \left([-(a \cdot s + e)]_q, \; a \right)$

$= (pk_0, pk_1)$

$[pk(s)]_q = pk_0 + pk_1 \cdot s = e \simeq 0$



$Enc_{pk}(m)$: $m \in R_t$

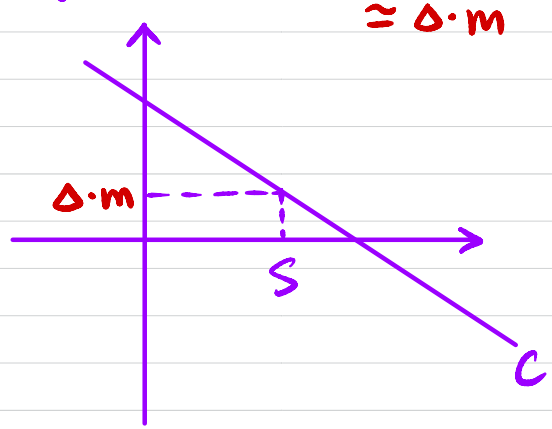
Sample $u, e_1, e_2 \leftarrow \chi$

$c = \left([pk_0 \cdot u + e_1 + \Delta \cdot m]_q, \; [pk_1 \cdot u + e_2]_q \right)$

$= (c_0, c_1)$

$[c(s)]_q = c_0 + c_1 \cdot s = -e \cdot u + e_1 + e_2 \cdot s + \Delta \cdot m$

$\simeq \Delta \cdot m$



$Dec_{sk}(c)$? $\quad c_0 + c_1 \cdot s \rightarrow \Delta \cdot m + \text{error}$

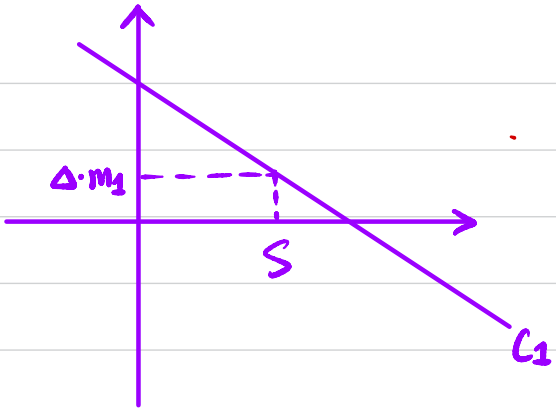
SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s = \Delta \cdot m + e$$

Homomorphism:

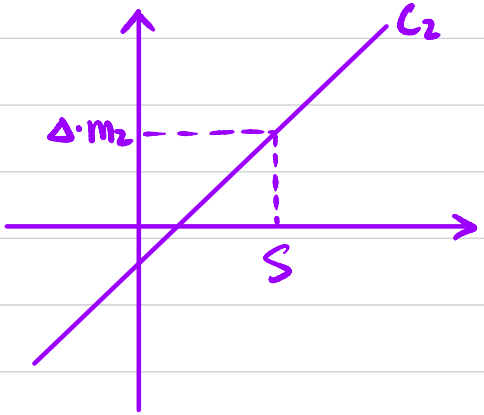
$$[C^{(1)}(s)]_q = \Delta \cdot m_1 + e_1$$

$$[C^{(2)}(s)]_q = \Delta \cdot m_2 + e_2$$



Additive Homomorphism?

$$[C^{(1)}(s) + C^{(2)}(s)]_q = [\Delta \cdot (m_1 + m_2) + e_1 + e_2]_q$$

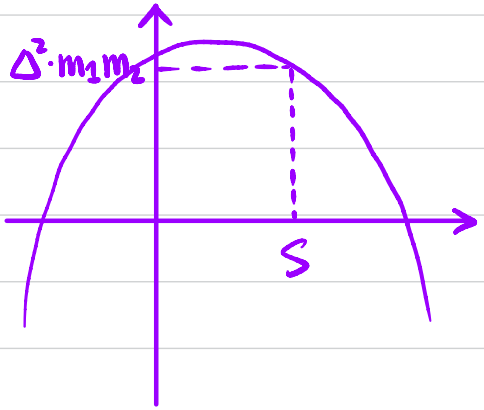


Multiplicative Homomorphism?

$$C^{(1)}(s) \cdot C^{(2)}(s)$$

$$= (\Delta \cdot m_1 + e_1 + \alpha_1 \cdot q) \cdot (\Delta \cdot m_2 + e_2 + \alpha_2 \cdot q)$$

$$= \left\lceil \left(\Delta^2 \cdot m_1 m_2 + \Delta m_1 e_2 + \Delta m_1 \cdot \alpha_2 q + e_1 \cdot \Delta m_2 + e_1 e_2 + e_1 \alpha_2 q + \alpha_1 q \Delta m_2 + \alpha_1 q e_2 + \alpha_1 \alpha_2 q^2 \right) \cdot \frac{t}{q} \right\rfloor$$



WANT: $\Delta \cdot m_1 m_2 + \text{small}$

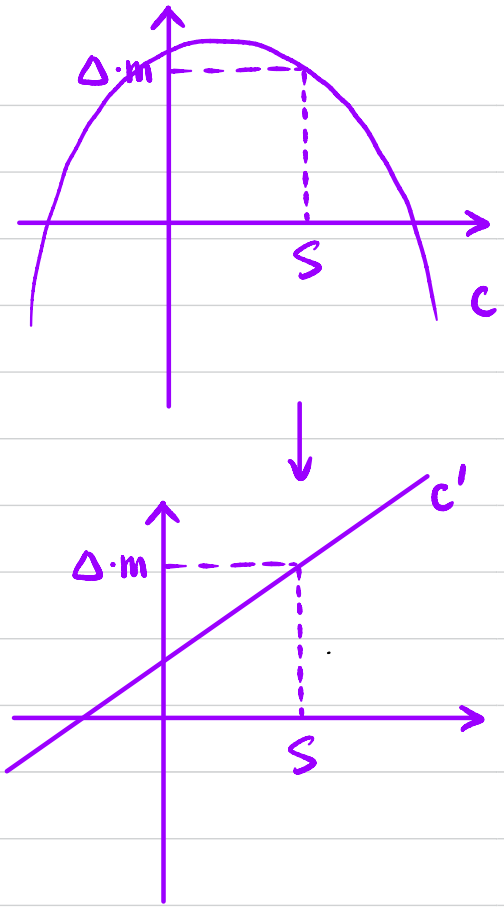
$$\Delta = \left\lfloor \frac{q}{t} \right\rfloor$$

SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s + c_2 \cdot s^2 = \Delta \cdot m + e$$

$$\downarrow$$

$$[C'(s)]_q = c_0' + c_1' \cdot s = \Delta \cdot m + e$$

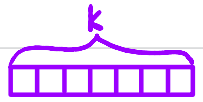


Relinearization:

Relinearization key:

part of pk → $rlk = \left([-(a \cdot s + e - s^2)]_q,\ a\right) = (rlk_0, rlk_1)$

$$[rlk(s)]_q = s^2 + \text{small}$$



$$c_0 + c_1 \cdot s + c_2 \cdot rlk(s) = c_0 + c_1 \cdot s + c_2 \cdot (s^2 + \text{small}) = \Delta \cdot m + e + c_2 \cdot \text{small}$$

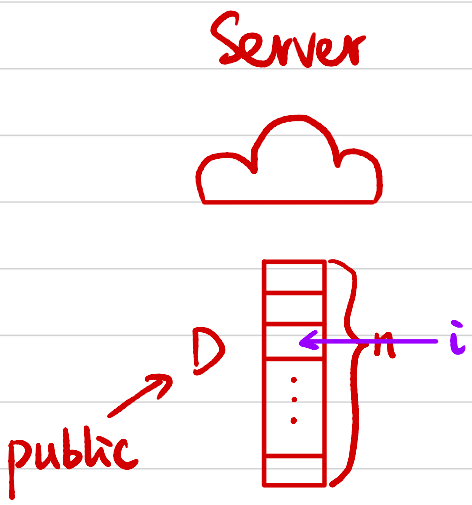
(c_2 · small: large)

$$\sum c_2[i] \cdot rlk_i(s) = \sum c_2[i] \cdot (z^i \cdot s^2 + e_i) = \sum c_2[i] \cdot z^i \cdot s^2 + \sum c_2[i] \cdot e_i$$

$$rlk_i = \left([-(a \cdot s + e_i - z^i \cdot s^2)]_q,\ a\right) \quad = c_2 \cdot s^2 + \text{small}$$

$$[rlk_i(s)]_q = z^i \cdot s^2 + e_i$$

Application: Private Information Retrieval (PIR)



WANT: D[i]

While hiding i against Server

Query i

Key sk

$ct \leftarrow Enc(i)$

ct ←

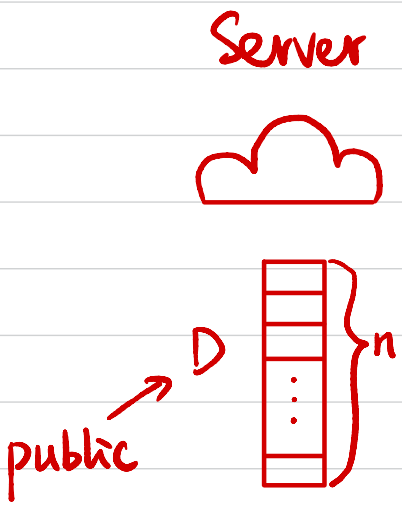
$ct' \leftarrow Eval(f, ct)$

$f_D(i) = D[i]$

→ ct'

$D[i] \leftarrow Dec_{sk}(ct')$

Private Information Retrieval (PIR)



WANT: D[i]

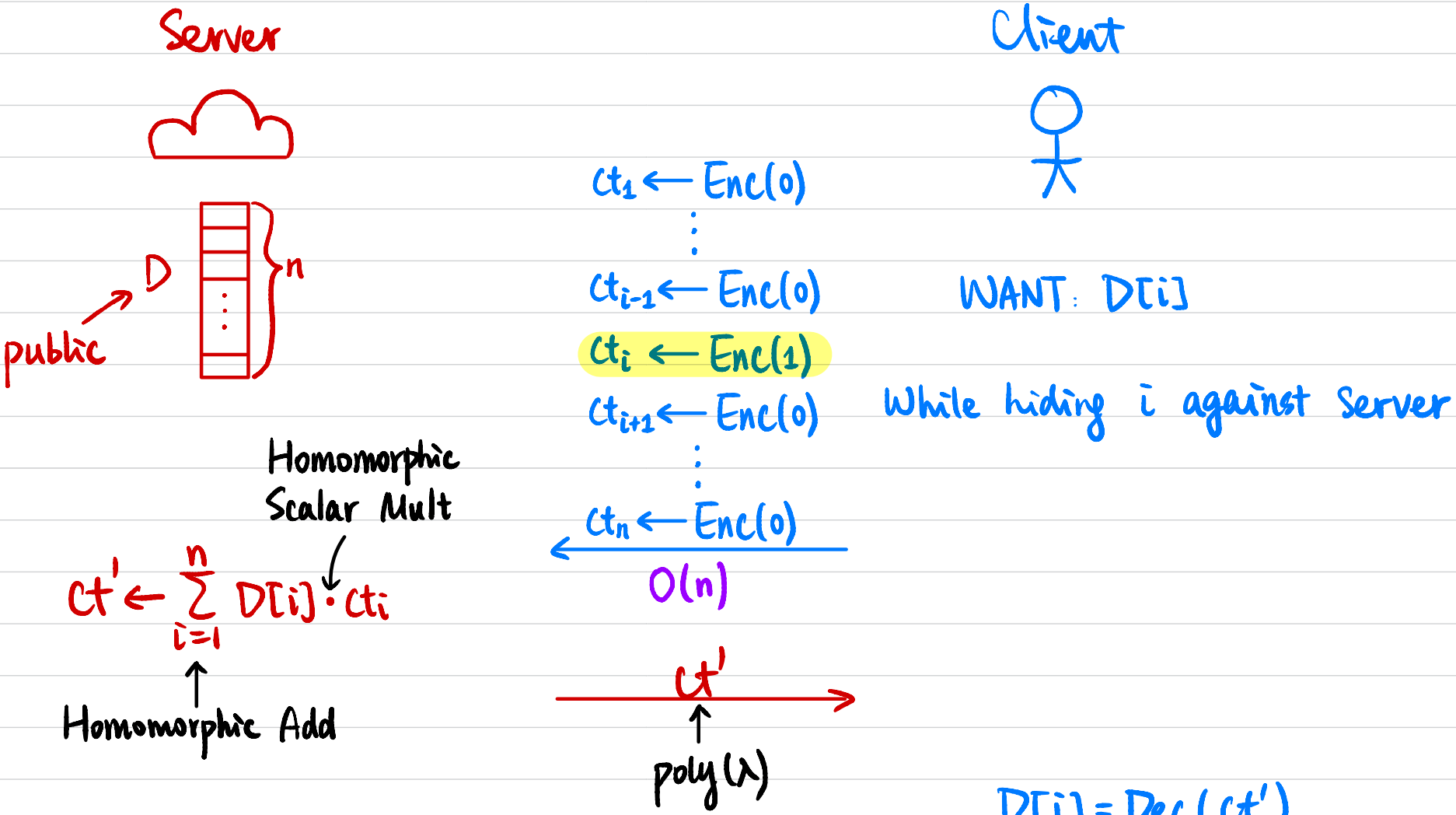
While hiding i against Server

Trivial Solution:

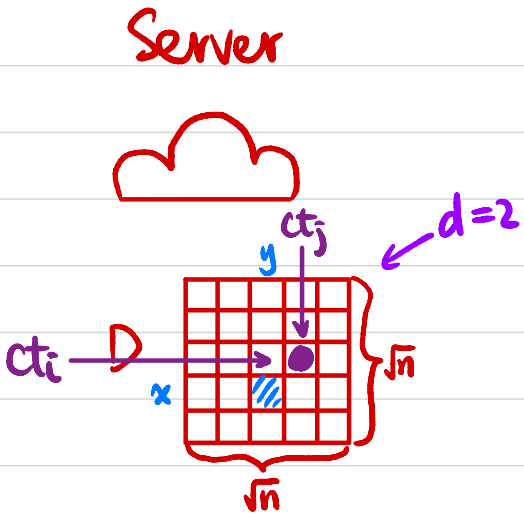
Communication complexity $O(n)$

Goal: Communication complexity $o(n)$

Private Information Retrieval (PIR)



Private Information Retrieval (PIR)



$$\underbrace{d_{\sqrt{n}} \times d_{\sqrt{n}} \times \cdots \times d_{\sqrt{n}}}_{d}$$

$O(2 \cdot \sqrt{n})$

$ct_1^{(2)} \leftarrow Enc(0)$ $\quad$ $ct_1^{(1)} \leftarrow Enc(0)$

$ct_{x-1}^{(1)} \leftarrow Enc(0)$ $\quad$ $ct_{y-1}^{(2)} \leftarrow Enc(0)$

$ct_x^{(2)} \leftarrow Enc(1)$ $\quad$ $ct_y^{(1)} \leftarrow Enc(1)$

$ct_{x+1}^{(1)} \leftarrow Enc(0)$ $\quad$ $ct_{y+1}^{(2)} \leftarrow Enc(0)$

$ct_{\sqrt{n}}^{(1)} \leftarrow Enc(0)$ $\quad$ $ct_{\sqrt{n}}^{(2)} \leftarrow Enc(0)$

WANT: $D[x,y]$

While hiding (x,y) against Server

↑ Why?

Homomorphic Scalar Mult

$$ct' \leftarrow \sum_{i,j=1}^{\sqrt{n}} D[i,j] \cdot ct_i^{(1)} \cdot ct_j^{(2)}$$

↑ Homomorphic Add

↑ Homomorphic Mult

ct' →

↑ $poly(\lambda)$

$D[x,y] = Dec(ct')$

↑ Why?

Extend to dimension d ?

Homomorphic Mult $= (d-1) \cdot n$

Homomorphic Scalar Mult $= n$

Homomorphic Add $= n-1$

Communication $= d \cdot n^{1/d}$

$\underbrace{2 \times 2 \times \cdots \times 2}_{\log_2 n} = n$